



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/650,440	08/27/2003	Frederic G. Thiele	END920030068US1	7247

26502 7590 03/05/2007
IBM CORPORATION
IPLAW IQ0A/40-3
1701 NORTH STREET
ENDICOTT, NY 13760

EXAMINER

PERUNGA VOOR, VENKATANARAY

ART UNIT	PAPER NUMBER
----------	--------------

2132

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/05/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary

Application No.

10/650,440

Applicant(s)

THIELE ET AL.

Examiner

Venkat Perungavoor

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 18 January 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-16 and 21-24 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-16 and 21-24 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

Response to Arguments

Applicant's arguments, see pages 11-14, filed 1/7/2007, with respect to the rejection(s) of claim(s) 1-24 under 35 USC § 102(e) as anticipated by US Patent Pub 2003/0145228 A1 to Suuronen et al. have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of US Patent Pub 2002/0116512 to Amit et al.(hereinafter Amit) in combination with US Patent Pub 2003/0145228 A1 to Suuronen et al.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-2,4-5, 13-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Publication 2003/0145228 A1 to Suuronen et al.(hereinafter Suuronen) in view of US Patent Publication 2002/0116512 to Amit et al.(hereinafter Amit).

Regarding Claim 1, 13, Suuronen discloses the computer storage medium see Abstract; first program to determine if packet is known exploit or portion thereof see Par. 0021; a third program to determine administration packet see Fig. 1 item 20(IP packets that cannot contain viruses, administration packets belong in this category). But fails to explicitly disclose the packet being addressed to a broadcast address and further to determine whether it is a new packet. However, Amit discloses the packet addressed to a broadcast address see Fig. 4 item "Receiving TCP connection data" and further of examining the packet to detect new packets see "Detect new connections requests". Further yet, Amit discloses the new packets being classified as primary(i.e. known and reliable source, axiomatic to benign of instant invention) and secondary(unknown source) see "Classifying new connection request as "secondary"" & "Classifying new connection request as "primary"". It would be obvious to one having ordinary skill in the art at the time of the invention to include packet being addressed to a broadcast address and further to determine whether it is a new packet in the invention of Suuronen in order to be able to download new packets as taught in Amit see Par. 0035.

Regarding Claim 2, 14, 22, Suuronen discloses the firewall being used for scanning for violation of rules and determination of web traffic including web crawlers and broadcast packets see Par. 0009 & Fig. 1. Suuronen discloses the dropping of packets from the Firewall(14) that do not comply with the rules, see Fig. 1. And packet being examined if the database can find it or otherwise considered new see Fig. 1 item 24.

Regarding Claim 4, 17, Suuronen discloses the blacklisting of packets so that known exploits can no longer have access to network's destination see Par. 0007.

Regarding Claim 5, 15, Suuronen discloses the gateway being used being several communication networks see Fig. 2-5, whereby the gateway is an computing device that is easily adaptable on an network and not a dedicated device.

Regarding Claim 7, Suuronen discloses the scanning of packets for signature see Fig. 1 item 22.

Regarding Claim 12, Suuronen discloses the packets being alerted when the packet is not a broadcast or administration, known exploit see Fig. 1.

Regarding Claim 21, Suuronen discloses the computer storage medium see Abstract; first program to determine of packet is known exploit or portion thereof see Par. 0021; a third program to determine administration packet see Fig. 1 item 20(IP packets that cannot contain viruses, administration packets belong in this category). But fails to explicitly disclose the packet being addressed to an broadcast address and further to analyzing the packets including protocols for valid protocols. However, Amit discloses the packet addressed to a broadcast address see Fig. 4 item "Receiving TCP connection data" and further of analyzing the packets including protocols for valid protocols see Par. 0029. It would be obvious to one having ordinary skill in the art at the

time of the invention to include packet being addressed to an broadcast address and further to determine whether it is a new packet in the invention of Suuronen in order to be able to download new packets as taught in Amit see Par. 0034.

Claims 3, 8-11, 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S Patent Publication 2003/0145228 A1 to Suuronen et al.(hereinafter Suuronen) in view of US Patent Publication 2002/0116512 to Amit et al.(hereinafter Amit) and further in view of U.S. Patent 6853619 to Grenot.

Regarding Claim 3, Suuronen does not disclose the searching based on signature for known exploits. However, Grenot discloses the searching based on signature for known exploits see Col 6 Ln 8-25. It would be obvious to one having ordinary skill in the art at the time of the invention to include the signature searching for known exploits in the invention of Suuronen in order to search based on an quantitative measure as taught in Col 8 Ln 48-52 of Grenot.

Regarding Claim 8, Suuronen does not disclose the examining of gateways and sub-net masks. However, Grenot discloses the examining of gateways and sub-net masks see Col 6 Ln 26-35. It would be obvious to one having ordinary skill in the art at the time of the invention to include the examining of gateways and sub-net masks in the invention of Suuronen in order to examining flows as taught in Grenot see Col 6 Ln 26-35.

Art Unit: 2132

Regarding Claim 9-11, 24, Suuronen does not disclose the comparing of IP addresses and protocols. However, Grenot discloses the comparing of IP addresses and protocols see Col 5 Ln 63-Col 6 Ln 3 & Col 3 Ln 13-23. It would be obvious to one having ordinary skill in the art at the time of the invention to include the in the comparing of IP addresses and protocols invention of Suuronen in order to have a first line of defense against an attack.

Claims 6, 16, 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Publication 2003/0145228 A1 to Suuronen et al. (hereinafter Suuronen) in view of US Patent Publication 2002/0116512 to Amit et al. (hereinafter Amit) further in view of US Patent Publication 2002/0131369 A1 to Hasegawa et al. (hereinafter Hasegawa).

Regarding Claim 6, 16, 23, Suuronen does not disclose the administrator being alerted and analysis result being reported. However, Hasegawa discloses the manager being alerted and result being reported see Fig. 1 item 1, DB2. It would be obvious to one having ordinary skill in the art at the time of the invention to include the manager being alerted and result being reported in the invention of Suuronen in order to manager may take a proactive approach to deal with the threat as taught in Hasegawa see Par. 0038-0043.

Conclusion

Art Unit: 2132

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

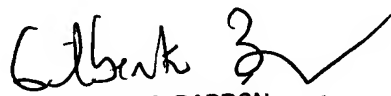
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Venkat Perungavoor whose telephone number is 571-272-7213. The examiner can normally be reached on 8:30-5:00. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2132

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Venkat Perungavoor
Examiner
Art Unit 2132

VP
3/1/2007


GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100